

# Intégration de Duo SAML SSO avec Anyconnect Secure Remote Access à l'aide de la posture ISE

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Diagramme du réseau](#)

[Flux de trafic](#)

[Configurations](#)

[- Configuration du portail d'administration Duo](#)

[- Configuration de la passerelle d'accès double \(DAG\)](#)

[- Configuration ASA](#)

[- Configuration ISE](#)

[Vérifier](#)

[Expérience utilisateur](#)

[Dépannage](#)

[Informations connexes](#)

---

## Introduction

Ce document décrit un exemple de configuration pour l'intégration de Duo SAML SSO avec l'accès client Cisco AnyConnect Secure Mobility Appliance (ASA) qui exploite Cisco ISE pour une évaluation détaillée de la position. Duo SAML SSO est mis en oeuvre à l'aide de la passerelle d'accès Duo (DAG) qui communique avec Active Directory pour l'authentification initiale de l'utilisateur, puis communique avec Duo Security (Cloud) pour l'authentification multifacteur. Cisco ISE est utilisé comme serveur d'autorisation pour la vérification des terminaux à l'aide de l'évaluation de la position.

Contribution de Dinesh Moudgil et Pulkit Saxena, Ingénieur HTTS de Cisco.

## Conditions préalables

### Exigences

Ce document suppose que l'ASA est entièrement opérationnel et configuré pour permettre à Cisco Adaptive Security Device Manager (ASDM) ou à l'interface de ligne de commande (CLI) d'apporter des modifications à la configuration.

Cisco vous recommande de prendre connaissance des rubriques suivantes :


- Notions de base sur la passerelle d'accès Duo et la sécurité Duo
- Connaissance de base de la configuration VPN d'accès à distance sur l'ASA
- Connaissances de base sur ISE et les services de posture

## Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Logiciel Cisco Adaptive Security Appliance Version 9.12(3)12
- Passerelle d'accès duo
- Sécurité Duo
- Cisco Identity Services Engine versions 2.6 et ultérieures
- Microsoft Windows 10 avec AnyConnect version 4.8.03052

---

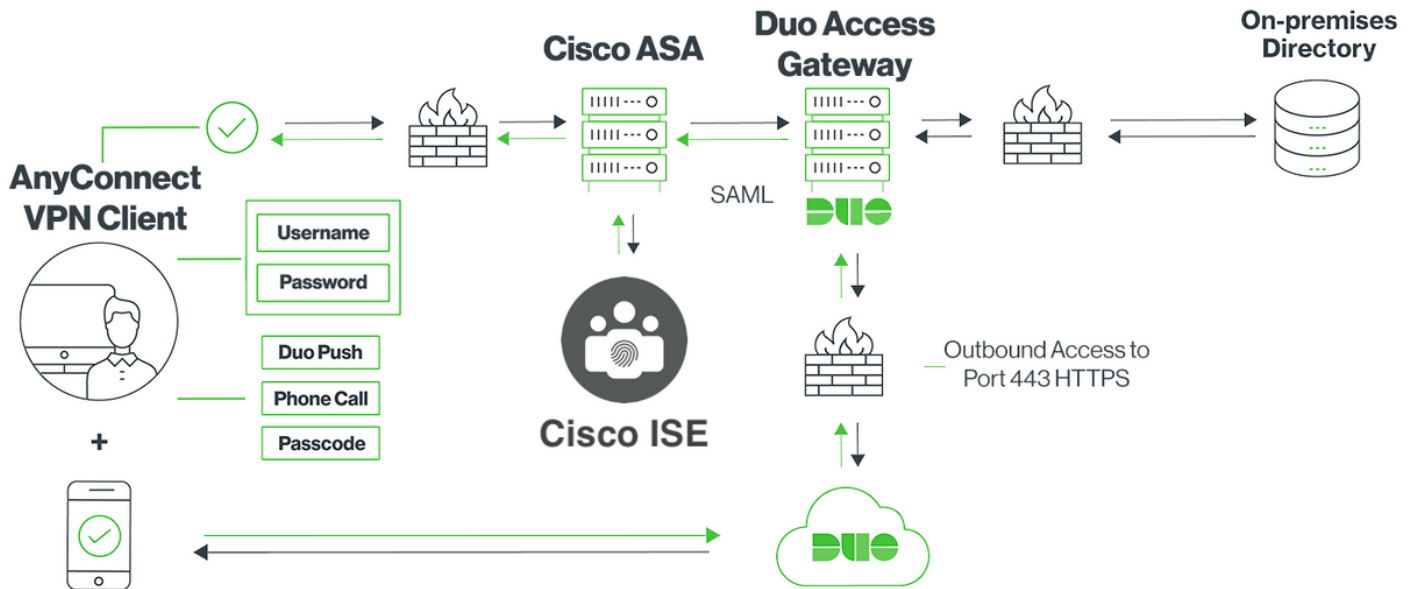
 Remarque : Anyconnect Embedded Browser, utilisé dans cette implémentation, nécessite ASA sur 9.7(1)24, 9.8(2)28, 9.9(2)1 ou version ultérieure de chaque version, et AnyConnect version 4.6 ou ultérieure.

---

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Configurer

### Diagramme du réseau



## Flux de trafic

1. Anyconnect client initie une connexion VPN SSL à Cisco ASA
2. Cisco ASA, configuré pour l'authentification principale avec Duo Access Gateway (DAG), redirige le navigateur intégré dans le client Anyconnect vers DAG pour l'authentification SAML
3. Le client Anyconnect est redirigé vers la passerelle d'accès duo
4. Une fois que le client AnyConnect a saisi les informations d'identification, une demande d'authentification SAML est créée et émise de Cisco ASA vers la passerelle d'accès Duo
5. Duo Access Gateway exploite l'intégration avec Active Directory sur site pour effectuer l'authentification principale pour le client Anyconnect
6. Une fois l'authentification principale réussie, la passerelle d'accès Duo envoie une requête à Duo Security sur le port TCP 443 pour commencer l'authentification à deux facteurs
7. Le client AnyConnect a affiché l'invite interactive Duo et l'utilisateur effectue l'authentification à deux facteurs Duo en utilisant la méthode de son choix (push ou code secret)
8. Duo Security reçoit une réponse d'authentification et renvoie les informations à la passerelle d'accès Duo
9. Sur la base de la réponse d'authentification, Duo Access Gateway crée une réponse d'authentification SAML qui contient une assertion SAML et répond au client Anyconnect
10. Le client Anyconnect s'authentifie correctement pour la connexion VPN SSL avec Cisco ASA
11. Une fois l'authentification réussie, Cisco ASA envoie une demande d'autorisation à Cisco



Remarque : Cisco ISE est configuré uniquement pour l'autorisation, car Duo Access Gateway fournit l'authentification nécessaire

---

12. Cisco ISE traite la demande d'autorisation et, puisque l'état de la position du client est Inconnu, renvoie la redirection de la position avec un accès limité au client Anyconnect via Cisco ASA
13. Si le client Anyconnect ne dispose pas d'un module de conformité, il est invité à le télécharger pour poursuivre l'évaluation de la position
14. Si le client Anyconnect dispose d'un module de conformité, il établit une connexion TLS avec Cisco ASA et le flux de posture démarre
15. Selon les conditions de posture configurées sur ISE, les vérifications de posture sont effectuées et les détails sont envoyés du client Anyconnect à Cisco ISE
16. Si l'état de la position du client passe de Inconnu à Conforme, une demande de modification d'autorisation (CoA) est envoyée de Cisco ISE à Cisco ASA pour accorder un accès complet au client et le VPN est entièrement établi

## Configurations

### - Configuration du portail d'administration Duo

Dans cette section, configurez l'application ASA sur le portail d'administration Duo.

1. Connectez-vous à « Duo Admin Portal » et naviguez jusqu'à « Applications > Protect an Application », et recherchez « ASA » avec le type de protection « 2FA with Duo Access Gateway, self-hosted ». Cliquez sur Protect (Protéger) à l'extrême droite pour configurer Cisco ASA

admin-77d04ebc.duosecurity.com/applications/protect/types

Search for users, groups, applications, or devices

Cisco | ID: 2010-1403-48 ciscoduobl

Dashboard > Applications > Protect an Application

## Protect an Application

ASA

Application	2FA	Single Sign-On (if available)	Documentation	Action
Asana	2FA	Duo Access Gateway (self-hosted)	<a href="#">Documentation</a>	<a href="#">Protect</a>
Cisco ASA	2FA	Duo Access Gateway (self-hosted)	<a href="#">Documentation</a>	<a href="#">Protect</a>
Cisco ASA	2FA	Single Sign-On (hosted by Duo)	<a href="#">Documentation</a>	<a href="#">Configure</a>

2. Configurez les attributs suivants sous « Fournisseur de services » pour l'application protégée ASA

URL de base	firebird.cisco.com
Groupe de tunnels	TG_SAML
Attribut de courrier	sAMAccountName,courrier

Cliquez sur « Enregistrer » en bas de la page

Device Insight

Policies

**Applications**

Protect an Application

Single Sign-On

Users

Groups

Endpoints

2FA Devices

Administrators

Reports

Settings

Billing

**Need Help?**

[Chat with Tech Support](#)

[Email Support](#)

Call us at 1-855-386-2884

**Account ID**  
2010-1403-48

**Deployment ID**  
DU057

**Helpful Links**  
[Documentation](#)

## Cisco ASA - Duo Access Gateway

Authentication Log | [Remove Application](#)

[Reset Secret Key](#)

### Configure Cisco ASA

To set up this application, install the Duo Access Gateway and then configure your service provider. [View Cisco ASA SAML SSO instructions](#)

Next step: [Download your configuration file](#)

#### Service Provider

**Base URL**   
Enter the Cisco ASA Base URL.

**Tunnel Group**   
Enter the Tunnel Group you are protecting with SSO.

**Custom attributes**  Use this setting if your Duo Access Gateway authentication source uses non-standard attribute names.

**Mail attribute**   
The attribute containing the email address of the user.

[Save Configuration](#)

Dans ce document, le reste de la configuration utilise des paramètres par défaut, mais ils peuvent être définis en fonction des exigences du client.

Des paramètres supplémentaires peuvent être ajustés pour la nouvelle application SAML à ce stade, comme la modification du nom de l'application à partir de la valeur par défaut, l'activation du libre-service ou l'attribution d'une stratégie de groupe.

3. Cliquez sur le lien « Download your configuration file » (Télécharger votre fichier de configuration) pour obtenir les paramètres de l'application Cisco ASA (sous la forme d'un fichier JSON). Ce fichier est téléchargé sur la passerelle d'accès Duo dans les étapes suivantes

Device Insight  
Policies  
**Applications**  
Protect an Application  
Single Sign-On  
Users  
Groups  
Endpoints  
2FA Devices  
Administrators  
Reports  
Settings  
Billing

Need Help?  
Chat with Tech Support  
Email Support  
Call us at 1-855-386-2884  
Account ID  
2010-1403-48  
Deployment ID  
DU057  
Helpful Links  
Documentation

## Cisco ASA - Duo Access Gateway

Authentication Log | Remove Application

### Configure Cisco ASA

Reset Secret Key

To set up this application, install the Duo Access Gateway and then configure your service provider. [View Cisco ASA SAML SSO instructions](#)

Next step: [Download your configuration file](#)

#### Service Provider

Base URL:   
Enter the Cisco ASA Base URL.

Tunnel Group:   
Enter the Tunnel Group you are protecting with SSO.

Custom attributes:  Use this setting if your Duo Access Gateway authentication source uses non-standard attribute names.

Mail attribute:   
The attribute containing the email address of the user.

Save Configuration

4. Sous « Tableau de bord > Applications », l'application ASA nouvellement créée ressemble à celle illustrée dans l'image ci-dessous :

admin-77d04ebc.duosecurity.com/applications

Cisco Study | Cisco Tools | Mix | SourceFire | VPN | AAA | ASA | IFT 6.7

Search for users, groups, applications, or devices

Cisco | ID: 2010-1403-48 | ciscoduobl

Dashboard > Applications

## Applications

SSO Setup Guide | Protect an Application

Export | Search

Name	Type	Application Policy	Group Policies
Cisco ASA - Duo Access Gateway	Cisco ASA - Duo Access Gateway		

1 total

5. Accédez à "Utilisateurs > Ajouter un utilisateur" comme indiqué dans l'image :

Créez un utilisateur nommé « duouser » à utiliser pour l'authentification Anyconnect Remote Access et activez Duo Mobile sur l'appareil de l'utilisateur final

Search for users, groups, applications, or devices

[Dashboard](#) > [Users](#) > [Add User](#)

## Add User

**Adding Users**  
Most applications allow users to enroll themselves after they complete primary authentication.  
[Learn more about adding users](#)

**Username**

Should match the primary authentication username.

[Add User](#)

Pour ajouter le numéro de téléphone tel qu'il apparaît sur l'image, sélectionnez l'option Ajouter un téléphone.

Search for users, groups, applications, or devices

[Dashboard](#) > [Users](#) > [duouser](#) > [Add Phone](#)

## Add Phone

[Learn more about Activating Duo Mobile](#)

**Type**  **Phone**  Tablet

**Phone number**  [Show extension field](#)

Optional. Example: "+91 91234 56789"

[Add Phone](#)

## Activer "Duo Mobile" pour l'utilisateur particulier

### Device Info

[Learn more about Activating Duo Mobile](#)



Not using Duo Mobile

[Activate Duo Mobile](#)




Model

Unknown

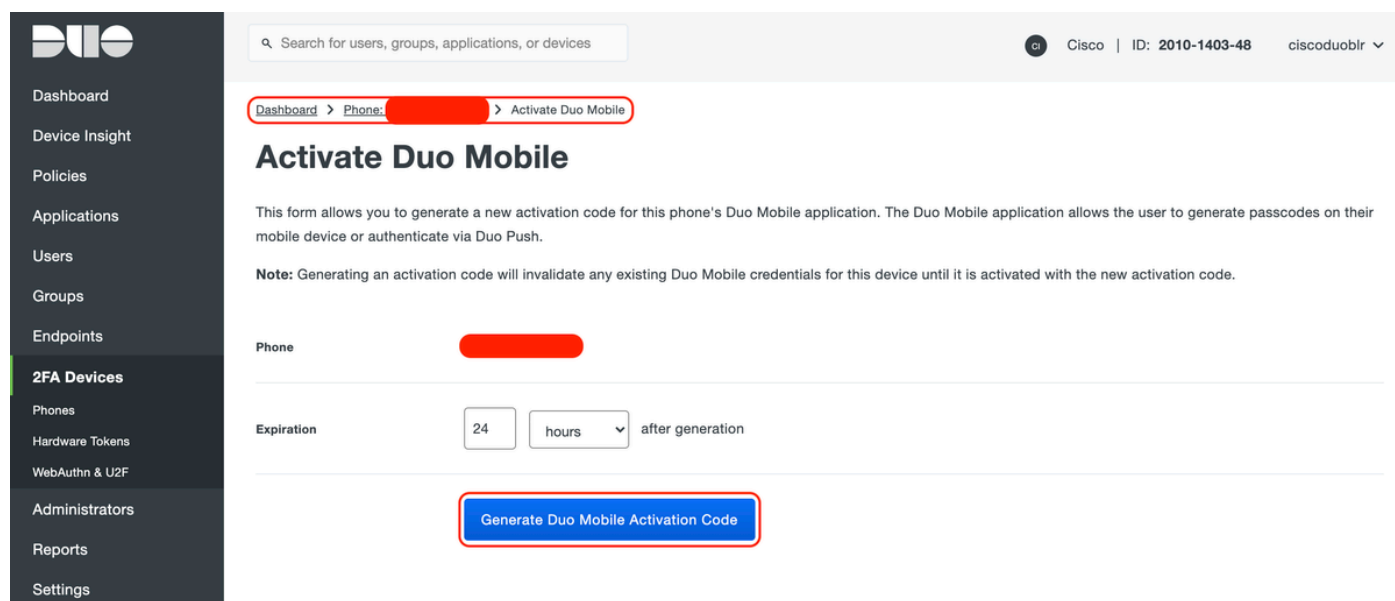


OS

Generic Smartphone

 Remarque : assurez-vous que Duo Mobile est installé sur l'appareil de l'utilisateur final.  
[Installation manuelle de l'application Duo pour les périphériques IOS](#)  
[Installation manuelle de l'application Duo pour les appareils Android](#)

Sélectionnez "Générer le code d'activation Duo Mobile" comme indiqué dans l'image :



Search for users, groups, applications, or devices

Cisco | ID: 2010-1403-48 | ciscodeubl

Dashboard > Phone: [redacted] > Activate Duo Mobile

### Activate Duo Mobile

This form allows you to generate a new activation code for this phone's Duo Mobile application. The Duo Mobile application allows the user to generate passcodes on their mobile device or authenticate via Duo Push.

**Note:** Generating an activation code will invalidate any existing Duo Mobile credentials for this device until it is activated with the new activation code.

Phone: [redacted]

Expiration: 24 hours after generation

[Generate Duo Mobile Activation Code](#)

Sélectionnez « Envoyer les instructions par SMS » comme indiqué dans l'image :



- Dashboard
- Device Insight
- Policies
- Applications
- Users
- Groups
- Endpoints
- 2FA Devices**
- Phones
- Hardware Tokens
- WebAuthn & U2F
- Administrators
- Reports
- Settings
- Billing
- Need Help?
- [Chat with Tech Support](#)
- [Email Support](#)
- Call us at 1-855-386-2884

[Dashboard](#) > [Phone: +91 \[redacted\]](#) > [Activate Duo Mobile](#)

# Activate Duo Mobile

A new Duo Mobile activation code has been generated, and any old credentials have been invalidated. activation instructions to the user by SMS.

Phone [redacted]

## Installation instructions

Send installation instructions via SMS

*Welcome to Duo! Please install Duo Mobile from your app store.*

## Activation instructions

Send activation instructions via SMS

*To activate the app, tap and open this link with Duo Mobile:  
<https://m-77d04ebc.duosecurity.com/activate/YB5ucEisJAq1YIBN5ZrT>*

[Send Instructions by SMS](#) or [skip this step](#)

Cliquez sur le lien dans le SMS, et l'application Duo est liée au compte d'utilisateur dans la section Device Info, comme le montre l'image :

The screenshot displays the Cisco Duo Mobile management console. On the left is a dark sidebar with navigation options: Dashboard, Device Insight, Policies, Applications, Users, Groups, Endpoints, 2FA Devices (highlighted), Phones, Hardware Tokens, WebAuthn & U2F, Administrators, Reports, Settings, Billing, and Need Help? (Chat with Tech Support). The main content area has a search bar at the top. Below it, a green banner indicates 'Duo Mobile instructions SMS'ed to +91 [redacted]'. A breadcrumb trail shows 'Dashboard > Phones > Phone: +91 [redacted]'. The phone number '+91 [redacted]' is prominently displayed. A 'Send SMS Passcodes...' button is visible. A 'Shared phone' section states 'This phone is attached to multiple users.' Below this, two user profiles are shown: 'duouser' and 'testing 123', both with phone numbers starting with '+91 [redacted]'. An 'Attach a user' link is present. A note states 'Authentication devices can share multiple users'. The 'Device Info' section includes a link to 'Learn more about Activating Duo Mobile', a 'Using Duo Mobile' button with a 'Reactivate Duo Mobile' link, a 'Model' field with the value 'Unknown', and an 'OS' field with the value 'Generic Smartphone'.

## - Configuration de la passerelle d'accès double (DAG)

1. Déployez la passerelle d'accès duo (DAG) sur un serveur de votre réseau

 Remarque : suivez les documents ci-dessous pour le déploiement :

Passerelle d'accès duo pour Linux

<https://duo.com/docs/dag-linux>

Passerelle d'accès duo pour Windows

<https://duo.com/docs/dag-windows>

2. Sur la page d'accueil de Duo Access Gateway, accédez à "Authentication Source"

3. Sous Configurer les sources, entrez les attributs suivants pour votre Active Directory et cliquez sur Enregistrer les paramètres

## Configure Sources

Configure authentication source settings below. Changes made to non-active authentication sources will take effect when made active.

Source type	<input type="text" value="Active Directory"/> Specify the authentication source to configure.
Status:	<span>✓ LDAP Bind Succeeded</span> <span>✓ ldap://10.197.243.110</span>
Server	<input type="text" value="10.197"/> <input type="text" value="389"/> Hostname and port of your Active Directory. The port is typically 389 for cleartext LDAP and STARTTLS, and 636 for LDAPS. Hostnames can be comma separated for failover functionality. For example: ad1.server.com,ad2.server.com,10.1.10.150
Transport type	<input checked="" type="radio"/> CLEAR <input type="radio"/> LDAPS <input type="radio"/> STARTTLS This setting controls whether the communication between Active Directory and the Duo Access Gateway is encrypted.
Attributes	<input type="text" value="sAMAccountName,mail"/> Specify attributes to retrieve from the AD server. For example: sAMAccountName,mail.
Search base	<input type="text" value="CN=Users,DC=dmoudgil,DC=local"/> The DNs which will be used as a base for the search. Enter one per line. They will be searched in the order given.
Search attributes	<input type="text" value="sAMAccountName"/> Specify attributes the username should match against. For example: sAMAccountName,mail.
Search username	<input type="text" value="iseadmin"/> The username of an account that has permission to read from your Active Directory. We recommend creating a service account that has read-only access.
Search password	<input type="password" value="••••"/> The password corresponding to the search username specified above.
<input type="button" value="Save Settings"/>	

4. Sous « Définir la source active », sélectionnez le type de source « Active Directory » et cliquez sur « Définir la source active »

### Set Active Source

Specify the source that end-users will use for primary authentication.

Source type

Active Directory

Set Active Source

5. Accédez à Applications, sous le sous-menu Add Application, téléchargez le fichier .json téléchargé depuis Duo Admin Console dans la section Configuration file. Le fichier .json correspondant a été téléchargé à l'étape 3 sous Duo Admin Portal Configuration

## Applications

### Add Application

Create a SAML application in the Duo Admin Panel. Then, download the provided configuration file and upload it here.



Configuration file

Browse... Cisco ASA - Duo Access Gateway.json

Upload

6. Une fois l'application ajoutée, elle apparaît dans le sous-menu « Applications »

### Applications

Name	Type	Logo	
Cisco ASA - Duo Access Gateway	Cisco ASA		 Delete

7. Sous le sous-menu « Métadonnées », téléchargez les métadonnées XML et le certificat IdP et notez les URL suivantes, configurées sur l'ASA ultérieurement

1. URL SSO
2. URL de déconnexion
3. ID entité
4. URL d'erreur

**Metadata** Recreate Certificate

Information for configuring applications with Duo Access Gateway. [Download XML metadata](#)

Certificate: /C=US/ST=MI/L=Ann Arbor/O=Duo Security, Inc. [Download certificate](#)

Expiration: 2030-04-30 18:57:14

SHA-1 Fingerprint: [REDACTED]

SHA-256 Fingerprint: [REDACTED]

SSO URL	<a href="https://explorer.cisco.com/dag/saml2/idp/SSOService.php">https://explorer.cisco.com/dag/saml2/idp/SSOService.php</a>
Logout URL	<a href="https://explorer.cisco.com/dag/saml2/idp/SingleLogoutSer">https://explorer.cisco.com/dag/saml2/idp/SingleLogoutSer</a>
Entity ID	<a href="https://explorer.cisco.com/dag/saml2/idp/metadata.php">https://explorer.cisco.com/dag/saml2/idp/metadata.php</a>
Error URL	<a href="https://explorer.cisco.com/dag/module.php/duosecurity/du">https://explorer.cisco.com/dag/module.php/duosecurity/du</a>

## -Configuration ASA

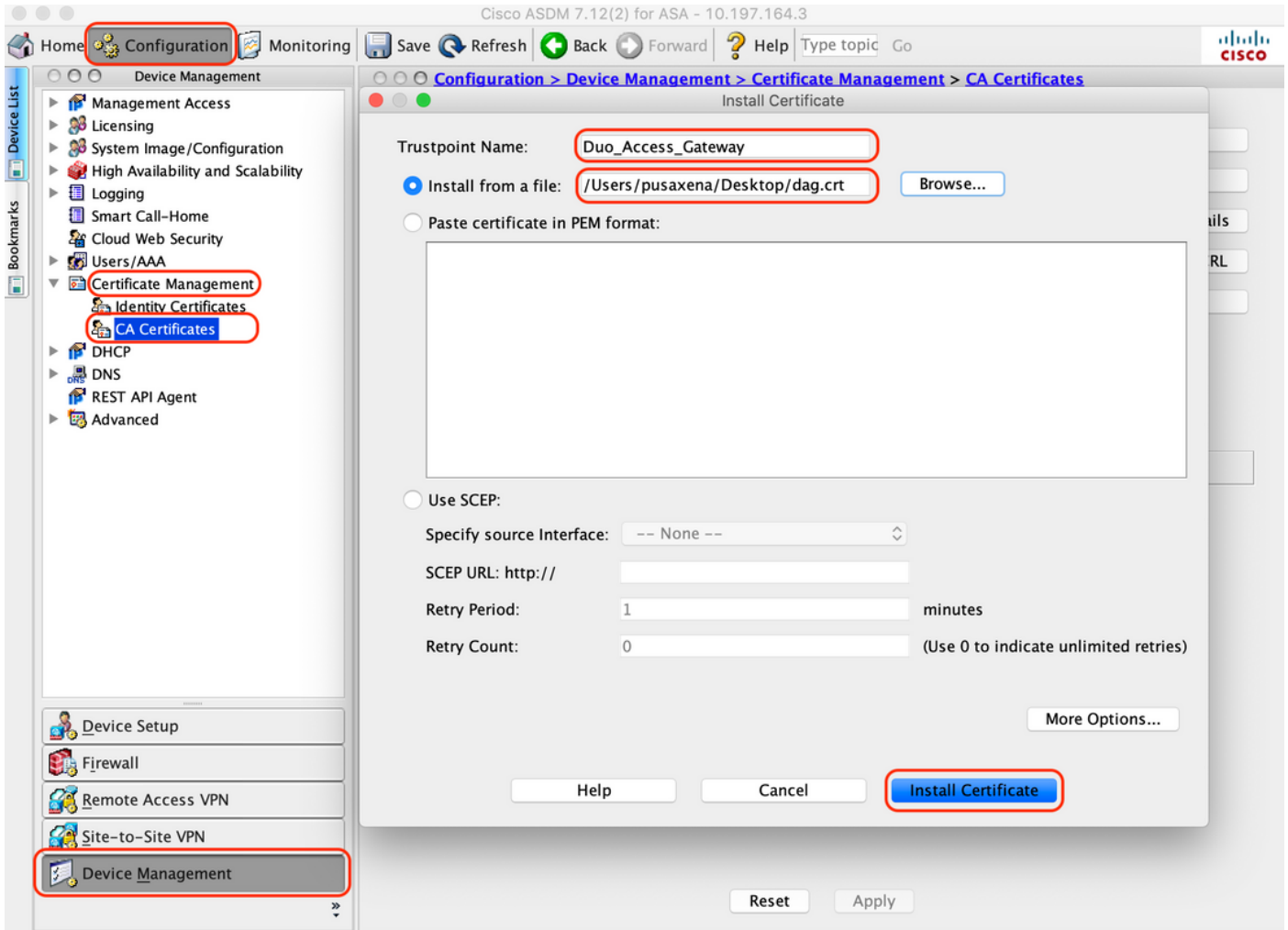
Cette section fournit des informations pour configurer ASA pour l'authentification SAML IDP et la configuration AnyConnect de base. Ce document présente les étapes de configuration ASDM et la configuration en cours de l'interface de ligne de commande.

1. Télécharger le certificat de passerelle d'accès duo

A. Accédez à Configuration > Device Management > Certificate Management > CA Certificates, cliquez sur Add

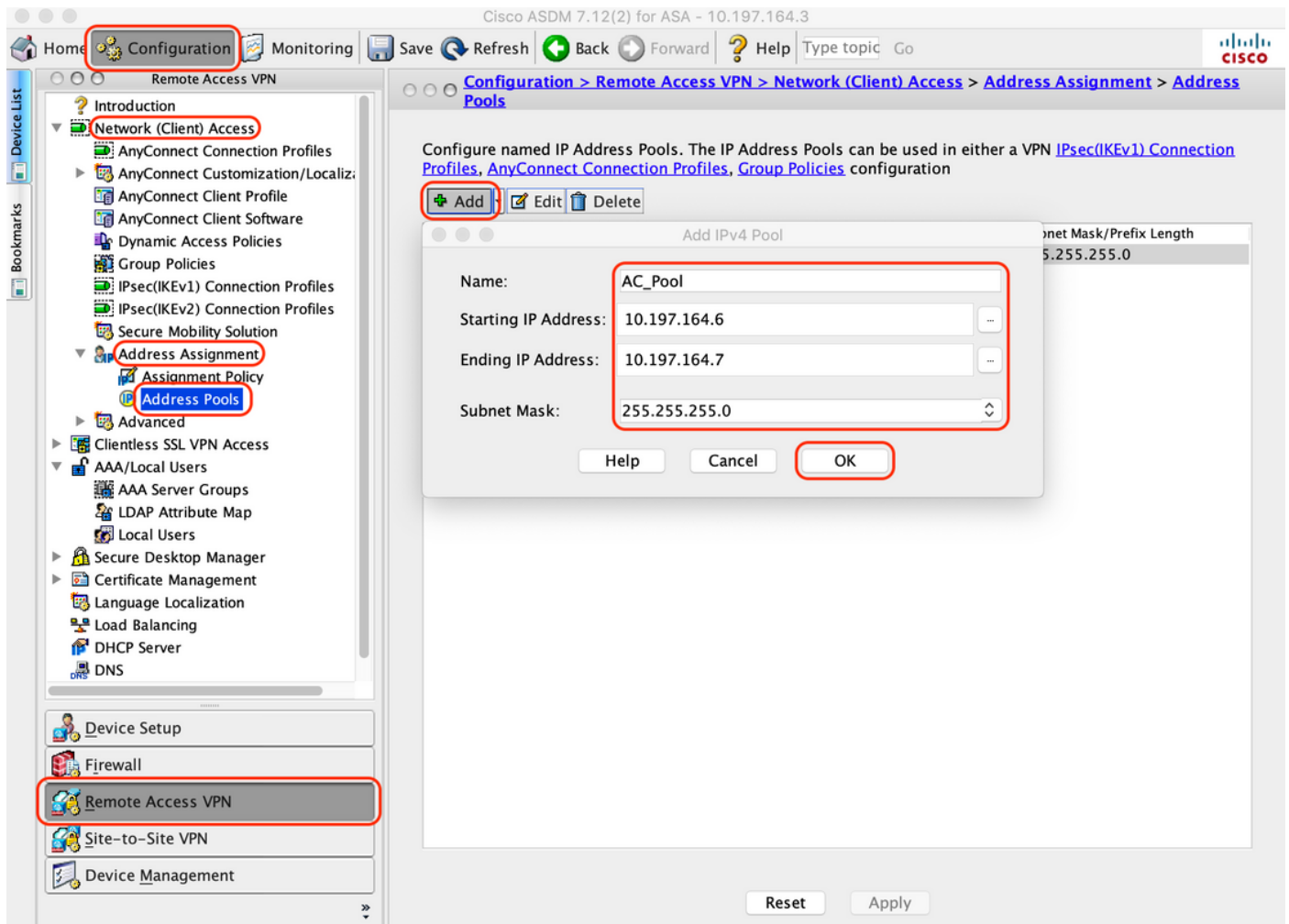
B. Sur la page « Install Certificate », configurez le nom du point de confiance : Duo\_Access\_Gateway

C. Cliquez sur « Parcourir » pour sélectionner le chemin associé au certificat DAG et, une fois sélectionné, cliquez sur « Installer le certificat »



## 2. Créer un pool local IP pour les utilisateurs AnyConnect

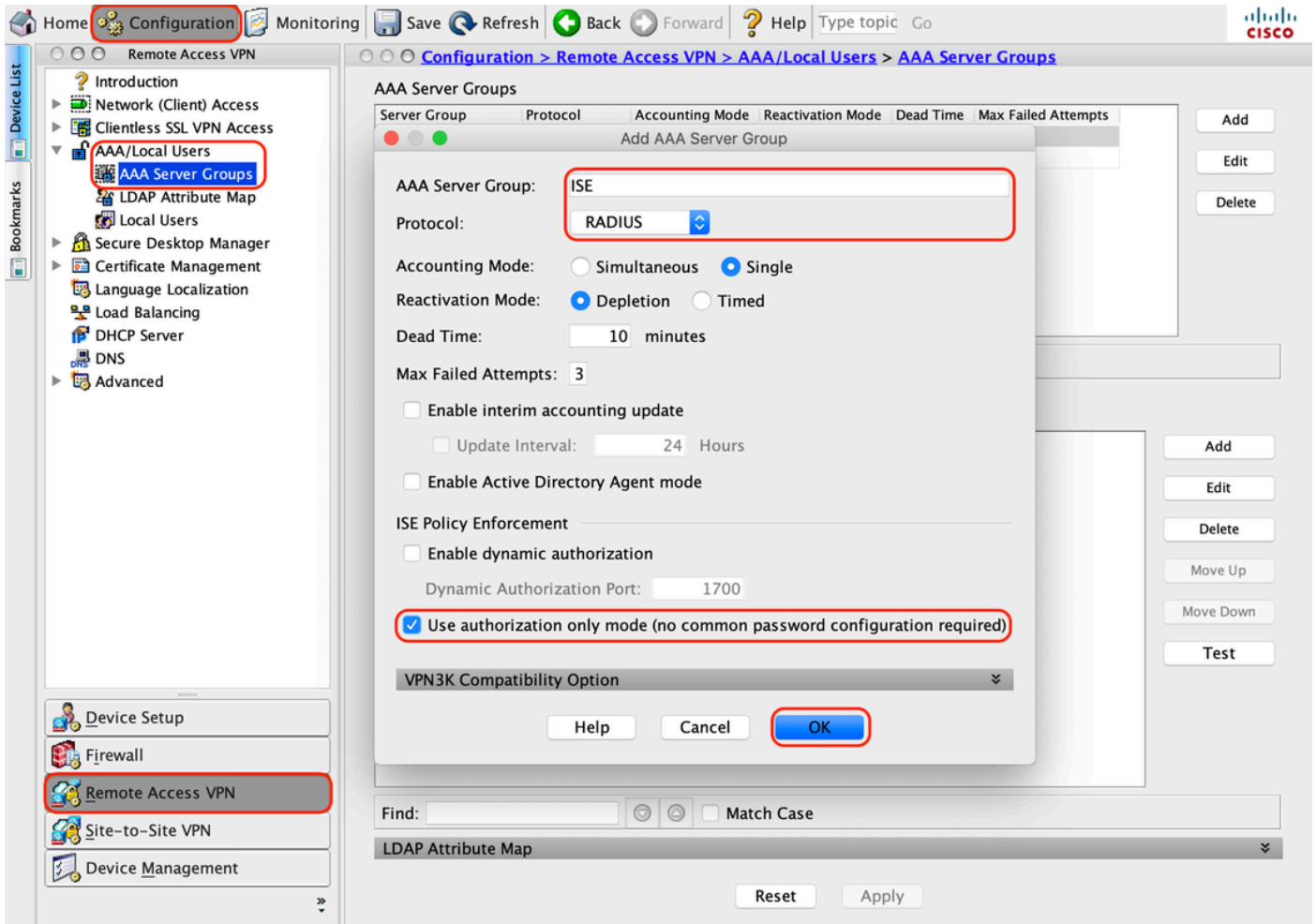
Accédez à "Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools", cliquez sur "Add"



### 3. Configurer le groupe de serveurs AAA

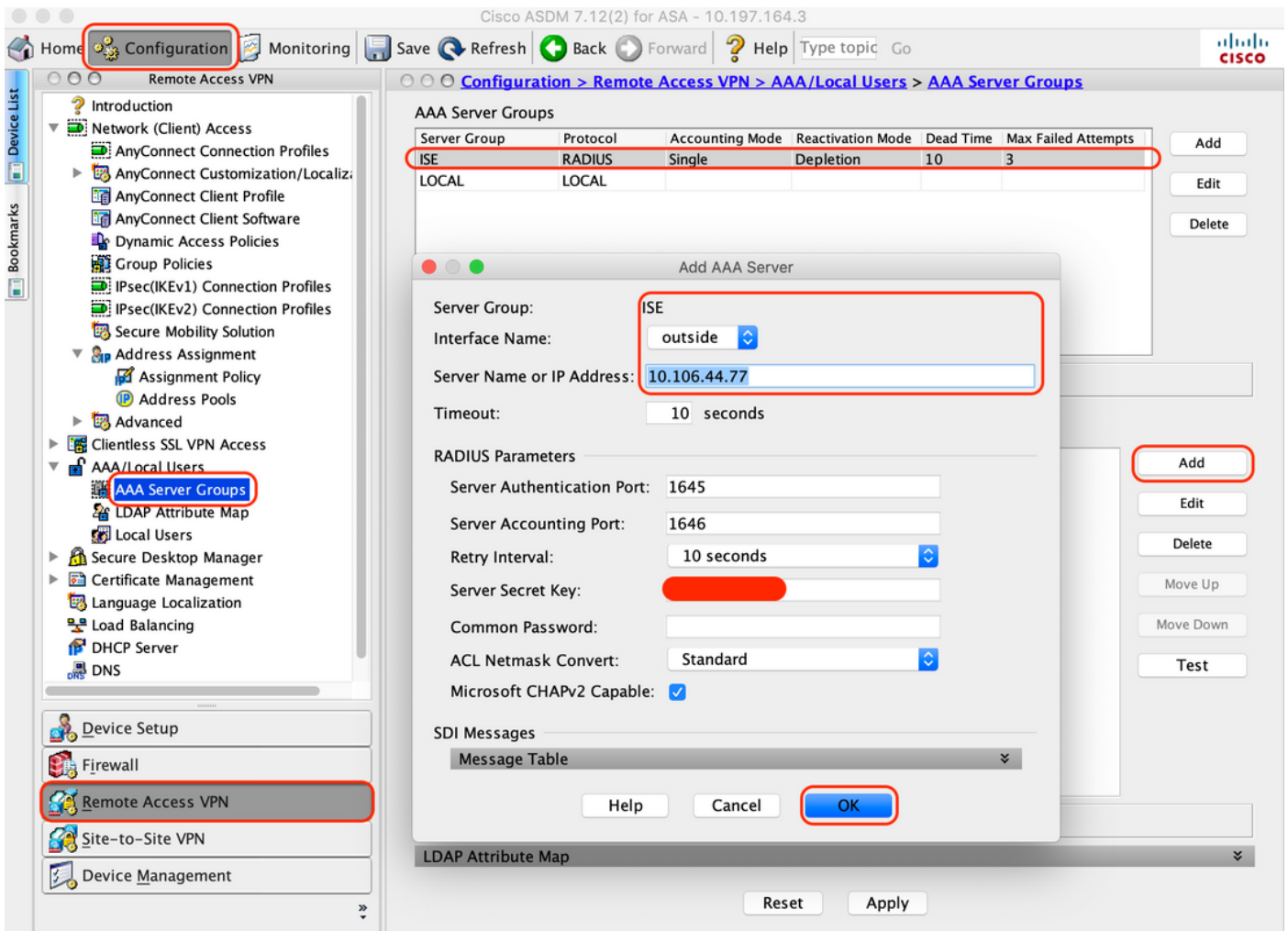
A. Dans cette section, configurez le groupe de serveurs AAA et fournissez des détails sur le serveur AAA spécifique qui effectue l'autorisation

B. Accédez à "Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups", cliquez sur "Add"



c. Sur la même page, sous la section « Serveurs dans le groupe sélectionné », cliquez sur « Ajouter » et fournissez les détails de l'adresse IP du serveur AAA

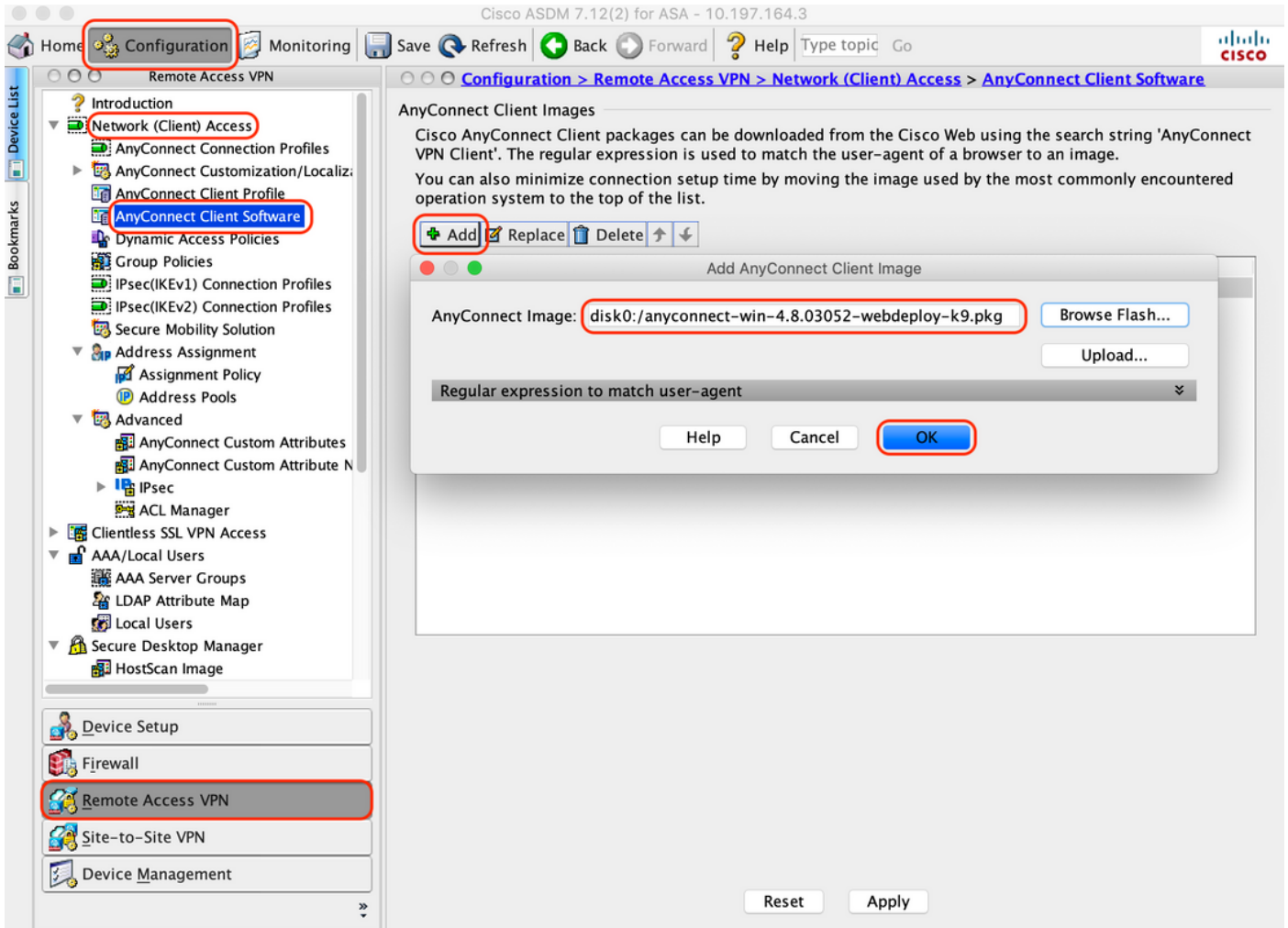




#### 4. Mappage du logiciel client AnyConnect

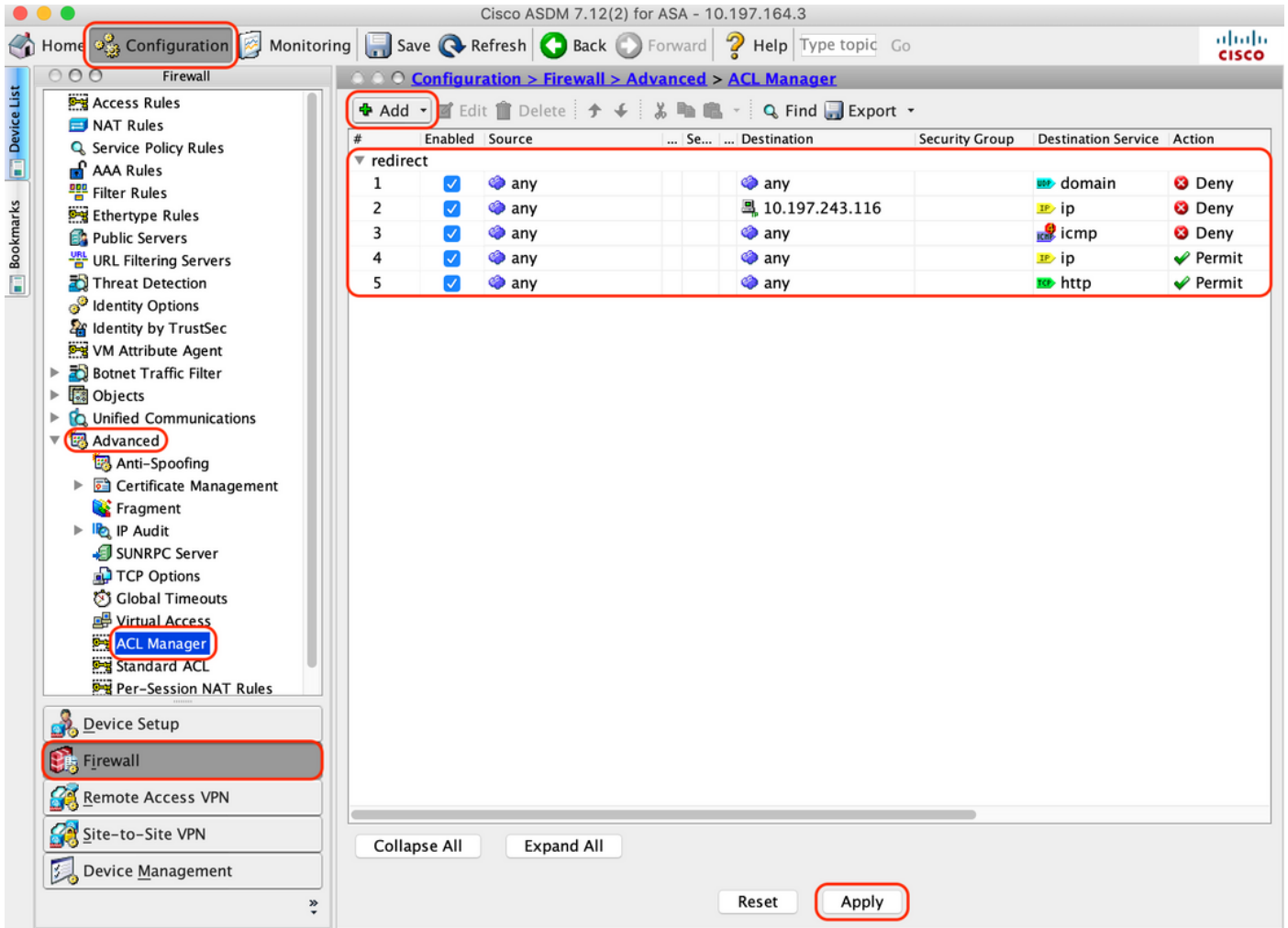
A. Mappez l'image de déploiement Web du logiciel client AnyConnect 4.8.03052 pour les fenêtres à utiliser pour WebVPN

B. Accédez à "Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Software", cliquez sur "Add"



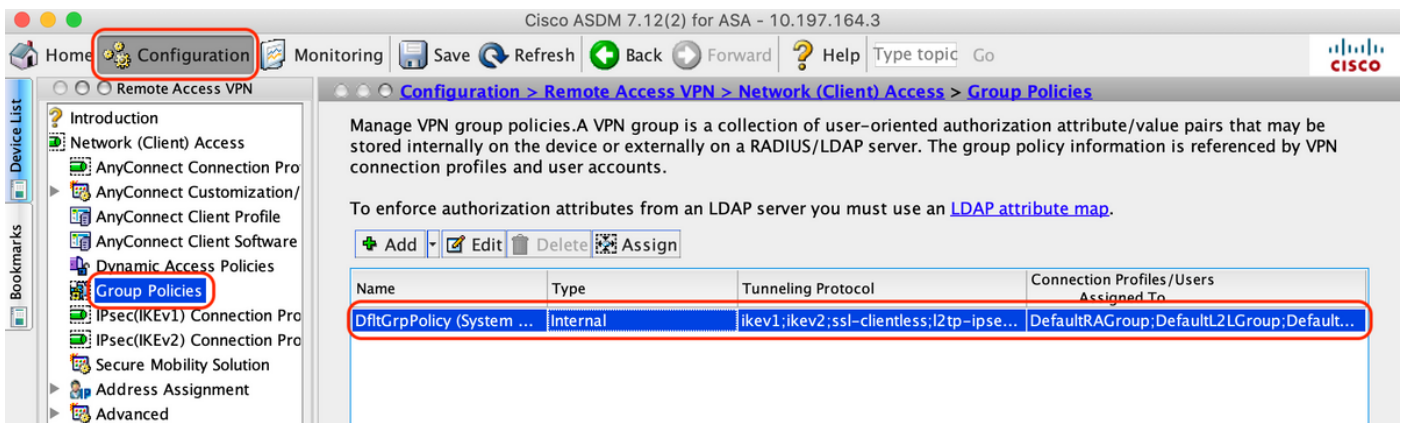
5. Configurez la liste de contrôle d'accès de redirection qui est transmise suite à ISE

A. Accédez à "Configuration > Firewall > Advanced > ACL Manager», cliquez sur Add pour ajouter l'ACL de redirection. Une fois configurées, les entrées apparaissent comme suit :



## 6. Valider la stratégie de groupe existante

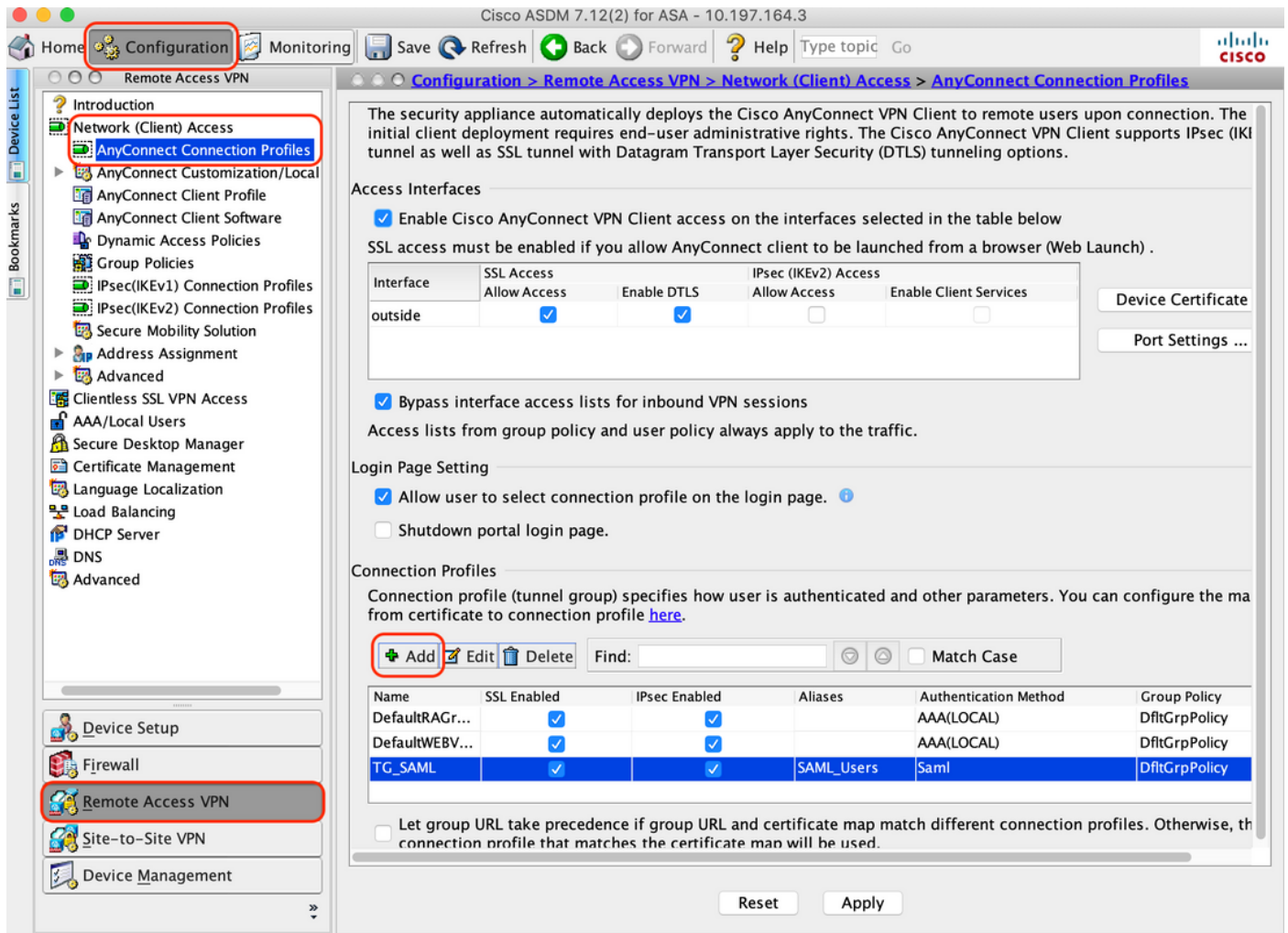
R. Cette configuration utilise la stratégie de groupe par défaut et peut être affichée à l'adresse : "Configuration > Remote Access VPN > Network (Client) Access > Group Policies"



## 7. Configurer le profil de connexion

A. Créer un nouveau profil de connexion auquel les utilisateurs AnyConnect se connectent

B. Accédez à "Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Connection Profiles", cliquez sur "Add"



C. Configurez les détails ci-dessous associés au profil de connexion :

Nom	TG_SAML
Alias	Utilisateurs_SAML
Méthode	SAML
Groupe de serveurs AAA	Municipal
Pools d'adresses client	AC_Pool
Stratégie de groupe	DfltGrpPolicy

Basic  
▶ Advanced

Name: TG\_SAML

Aliases: SAML\_Users

Authentication

Method: SAML

AAA Server Group: LOCAL Manage...

Use LOCAL if Server Group fails

SAML Identity Provider

SAML Server : <https://explorer.cisco.com/dag/saml2/idp/metadata.php> Manage...

Client Address Assignment

DHCP Servers:

None  DHCP Link  DHCP Subnet

Client Address Pools: AC\_Pool Select...

Client IPv6 Address Pools: Select...

Default Group Policy

Group Policy: DfltGrpPolicy Manage...

(Following fields are linked to attribute of the group policy selected above.)

Enable SSL VPN client protocol

Enable IPsec(IKEv2) client protocol

DNS Servers:

WINS Servers:

Domain Name:

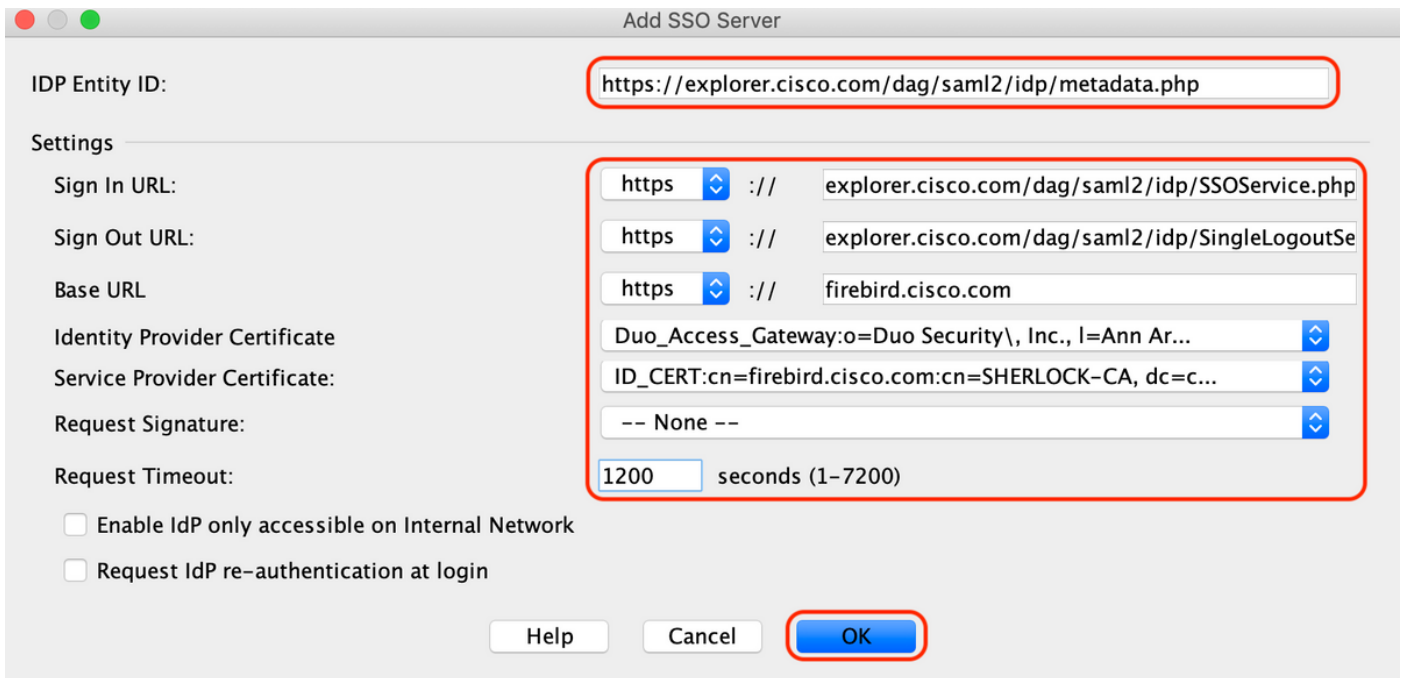
Find: Next Previous

Help Cancel OK

d. Sur la même page, configurez les détails du fournisseur d'identité SAML qui apparaissent comme suit :

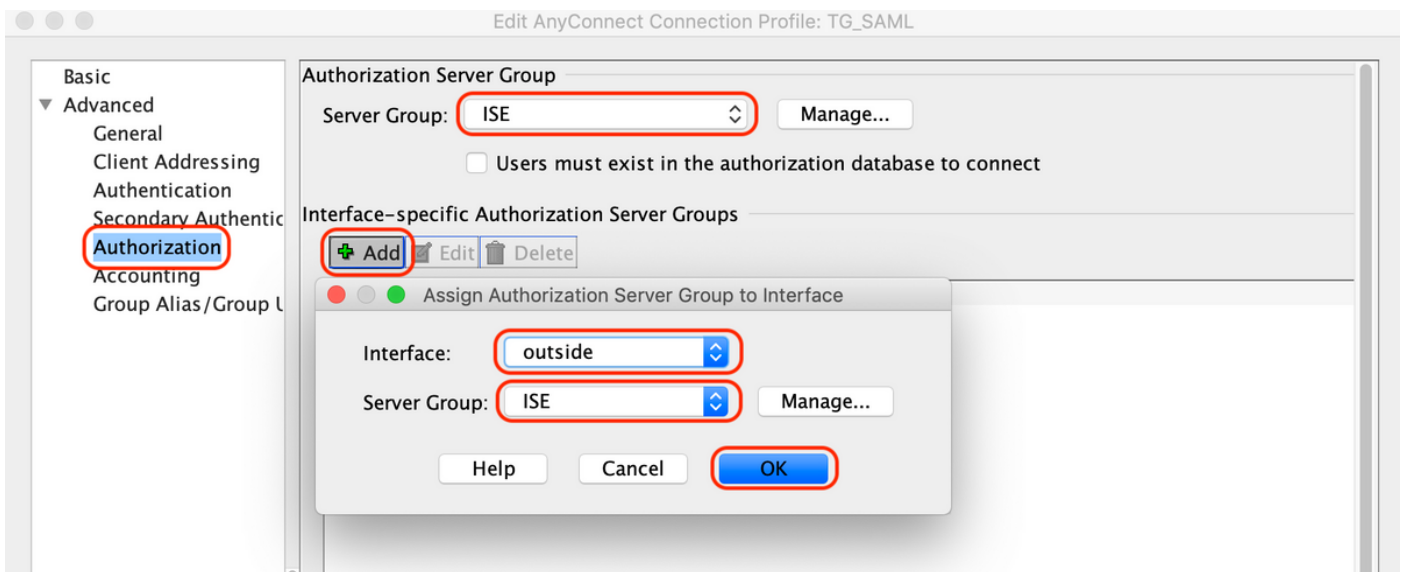
ID d'entité IDP	<a href="https://explorer.cisco.com/dag/saml2/idp/metadata.php">https://explorer.cisco.com/dag/saml2/idp/metadata.php</a>
URL de connexion	<a href="https://explorer.cisco.com/dag/saml2/idp/SSOService.php">https://explorer.cisco.com/dag/saml2/idp/SSOService.php</a>
URL de déconnexion	<a href="https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explorer.cisco.com/dag/saml2/idp/SSOService.php">https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explorer.cisco.com/dag/saml2/idp/SSOService.php</a>
URL de base	<a href="https://firebird.cisco.com">https://firebird.cisco.com</a>

E. Cliquez sur "Gérer > Ajouter"



F. Dans la section Advanced du profil de connexion, définissez le serveur AAA pour l'autorisation

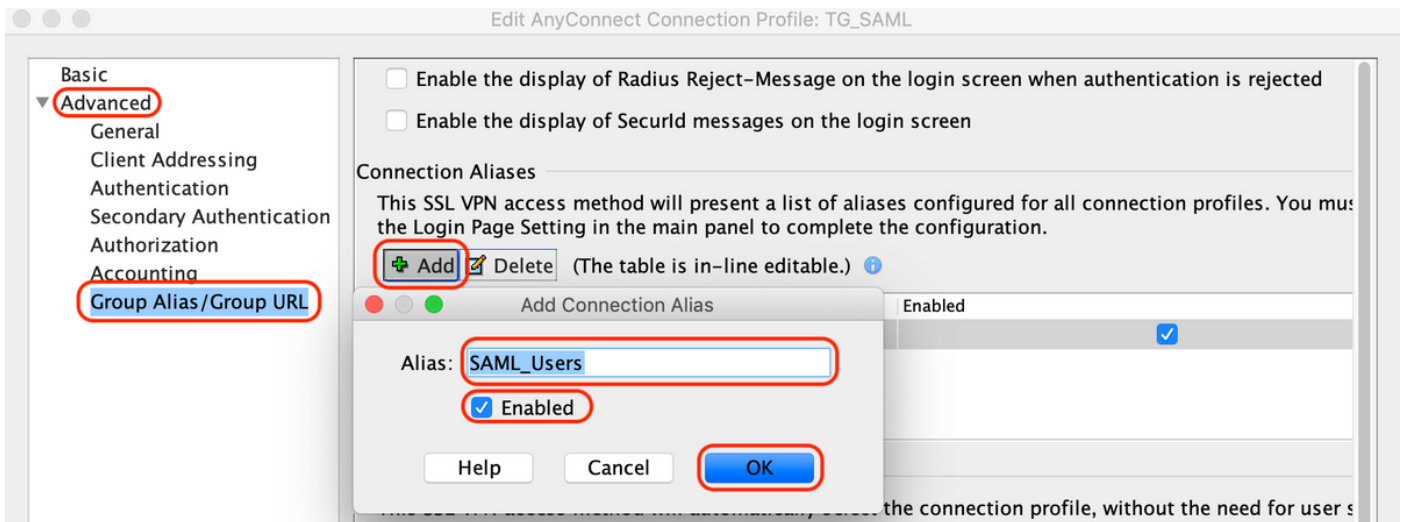
Accédez à "Avancé > Autorisation" et cliquez sur "Ajouter"



G. Sous Alias de groupe, définissez l'alias de connexion

Accédez à "Avancé > Alias de groupe/URL de groupe" et cliquez sur "Ajouter"





H. Ceci termine la configuration ASA, la même chose que ci-dessous sur l'interface de ligne de commande (CLI)

```

!
hostname firebird
domain-name cisco.com
!
!
name 10.197.164.7 explorer.cisco.com
name 10.197.164.3 firebird.cisco.com
!
!-----Client pool configuration-----
!
ip local pool AC_Pool 10.197.164.6-explorer.cisco.com mask 255.255.255.0
!
!-----Redirect Access-list-----
!
access-list redirect extended deny udp any any eq domain
access-list redirect extended deny ip any host 10.197.243.116
access-list redirect extended deny icmp any any
access-list redirect extended permit ip any any
access-list redirect extended permit tcp any any eq www
!
!-----AAA server configuration-----
!
aaa-server ISE protocol radius
  authorize-only
  interim-accounting-update periodic 1
  dynamic-authorization
aaa-server ISE (outside) host 10.106.44.77
  key *****
!
!-----Configure Trustpoint for Duo Access Gateway Certificate-----
!
crypto ca trustpoint Duo_Access_Gateway
  enrollment terminal
  crl configure
!
!-----Configure Trustpoint for ASA Identity Certificate-----
!
crypto ca trustpoint ID_CERT
  enrollment terminal
  fqdn firebird.cisco.com

```

```

subject-name CN=firebird.cisco.com
ip-address 10.197.164.3
keypair ID_RSA_KEYS
no ca-check
cr1 configure
!
!-----Enable AnyConnect and configuring SAML authentication-----
!
webvpn
enable outside
hsts
enable
max-age 31536000
include-sub-domains
no preload
anyconnect image disk0:/anyconnect-win-4.8.03052-webdeploy-k9.pkg 1
anyconnect enable
saml idp https://explorer.cisco.com/dag/saml2/idp/metadata.php
url sign-in https://explorer.cisco.com/dag/saml2/idp/SSOService.php
url sign-out https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explor
base-url https://firebird.cisco.com
trustpoint idp Duo_Access_Gateway
trustpoint sp ID_CERT
no signature
no force re-authentication
timeout assertion 1200
tunnel-group-list enable
cache
disable
error-recovery disable
!
!-----Group Policy configuration-----
!
group-policy DfltGrpPolicy attributes
vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless
!
!-----Tunnel-Group (Connection Profile) Configuraiton-----
!
tunnel-group TG_SAML type remote-access
tunnel-group TG_SAML general-attributes
address-pool AC_Pool
authorization-server-group ISE
accounting-server-group ISE
tunnel-group TG_SAML webvpn-attributes
authentication saml
group-alias SAML_Users enable
saml identity-provider https://explorer.cisco.com/dag/saml2/idp/metadata.php
!

```

## -Configuration ISE

### 1. Ajouter Cisco ASA en tant que périphérique réseau

Sous Administration > Network Resources > Network Devices, cliquez sur Add. Configurez le nom du périphérique réseau, l'adresse IP associée et sous « Paramètres d'authentification Radius », configurez le « Secret partagé » et cliquez sur « Enregistrer »



Network Devices

\* Name   
Description

IP Address  /

\* Device Profile    
Model Name   
Software Version

\* Network Device Group

Location    
IPSEC    
Device Type



▼ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**  
\* Shared Secret    
Use Second Shared Secret    
  
CoA Port

RADIUS DTLS Settings

DTLS Required    
Shared Secret    
CoA Port    
Issuer CA of ISE Certificates for CoA    
DNS Name

General Settings

Enable KeyWrap    
\* Key Encryption Key    
\* Message Authenticator Code Key    
Key Input Format  ASCII  HEXADECIMAL



▶ TACACS Authentication Settings



▶ SNMP Settings



▶ Advanced TrustSec Settings

## 2. Installez les dernières mises à jour de posture

Accédez à "Administration > System > Settings > Posture > Updates" et cliquez sur "Update Now"

### Posture Updates

Web  Offline

\* Update Feed URL

Proxy Address  ⓘ

Proxy Port  HH MM SS

Automatically check for updates starting from initial delay    every  hours ⓘ

### ▼ Update Information

Last successful update on	2020/05/07 15:15:05 ⓘ
Last update status since ISE was started	No update since ISE was started. ⓘ
Cisco conditions version	224069.0.0.0
Cisco AV/AS support chart version for windows	171.0.0.0
Cisco AV/AS support chart version for Mac OSX	91.0.0.0
Cisco supported OS version	41.0.0.0

## 3. Téléchargez le module de conformité et le package de déploiement de tête de réseau AnyConnect sur ISE

Accédez à "Policy > Policy Elements > Results > Client Provisioning > Resources". Cliquez sur Ajouter et sélectionnez Ressources d'agent à partir du disque local ou Ressources d'agent à partir du site Cisco selon que les fichiers doivent être récupérés à partir de la station de travail locale ou du site Cisco.

Dans ce cas, pour télécharger des fichiers à partir d'une station de travail locale sous Catégorie, sélectionnez « Packages fournis par Cisco », cliquez sur « Parcourir », sélectionnez les packages requis et cliquez sur « Envoyer ».

Ce document utilise « anyconnect-win-4.3.1012.6145-isecompliance-webdeploy-k9.pkg » comme module de conformité et « anyconnect-win-4.8.03052-webdeploy-k9.pkg » comme package de

déploiement de tête de réseau AnyConnect.

[Agent Resources From Local Disk](#) > [Agent Resources From Local Disk](#)

### Agent Resources From Local Disk

Category  ⓘ

Browse...

#### ▼ AnyConnect Uploaded Resources

Name	Type	Version	Description
AnyConnectDesktopWindows 4.8.30...	AnyConnectDesktopWindows	4.8.3052.0	AnyConnect Secure Mobility Clie...

#### 4. Créer un profil de position AnyConnect

A. Accédez à "Policy > Policy Elements > Results > Client Provisioning > Resources". Cliquez sur Ajouter et sélectionnez Profil de posture AnyConnect

B. Entrez le nom du profil de posture Anyconnect et configurez le nom du serveur en tant que « \* » sous les règles de nom du serveur, puis cliquez sur « Enregistrer »

### ISE Posture Agent Profile Settings > Anyconnect Posture Profile

\* Name:

Description:

## Posture Protocol

Parameter	Value	Notes	Description
PRA retransmission time	<input type="text" value="120"/> secs		This is the agent retry period if there is a Passive Reassessment communication failure
Retransmission Delay	<input type="text" value="60"/> secs	Default Value: 60. Acceptable Range between 5 to 300. Accept only integer Values.	Time (in seconds) to wait before retrying.
Retransmission Limit	<input type="text" value="4"/>	Default value: 4. Acceptable Range between 0 to 10. Accept only integer Values.	Number of retries allowed for a message.
Discovery host	<input type="text"/>	IPv4 or IPv6 addresses or FQDNs. IPv6 address should be without square brackets[]	The server that the agent should connect to
Server name rules	<input type="text" value="*"/>	need to be blank by default to force admin to enter a value. "*" means agent will connect to all	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. "*.cisco.com"
Call Home List	<input type="text"/>	List of IPv4 or IPv6 addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port. Example: IPaddress/FQDN:Port (Port number should be the same, specified in the Client Provisioning portal)	A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.
Back-off Timer	<input type="text" value="30"/> secs	Enter value of back-off timer in seconds, the supported range is between 10s - 600s.	Anyconnect agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached

## 5. Créer une configuration Anyconnect

A. Accédez à "Policy > Policy Elements > Results > Client Provisioning > Resources". Cliquez sur Ajouter et sélectionnez Configuration AnyConnect.

B. Sélectionnez le package AnyConnect, saisissez le nom de la configuration, puis sélectionnez le module de conformité requis

C. Sous « Sélection du module AnyConnect », cochez « Outil de diagnostic et de création de rapports »

D. Sous "Profile Selection", sélectionnez Posture Profile et cliquez sur "Save"

\* Select AnyConnect Package **AnyConnectDesktopWindows 4.8.3052.0** ▼

\* Configuration Name **AnyConnect Configuration**

Description:

**DescriptionValue**

\* Compliance Module **AnyConnectComplianceModuleWindows 4.3.1250.614** ▼

Notes

**AnyConnect Module Selection**

ISE Posture

VPN

Network Access Manager

Web Security

AMP Enabler

ASA Posture

Network Visibility

Umbrella Roaming Security

Start Before Logon

**Diagnostic and Reporting Tool**

**Profile Selection**

\* ISE Posture **Anyconnect Posture Profile** ▼

VPN ▼

Network Access Manager ▼

Web Security ▼

AMP Enabler ▼

Network Visibility ▼

Umbrella Roaming Security ▼

Customer Feedback ▼

6. Créer une politique de provisionnement client

A. Accédez à "Policy > Client Provisioning"

B. Cliquez sur Modifier, puis sélectionnez Insérer une règle ci-dessus

C. Saisissez le nom de la règle, sélectionnez le système d'exploitation requis, puis sous Résultats (dans Agent > Configuration de l'agent ), sélectionnez Configuration AnyConnect créée à l'étape 5 et cliquez sur Enregistrer

**Client Provisioning Policy**

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:  
 For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.  
 For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
IOS	If Any	and Apple iOS All	and Condition(s)	then Cisco-ISE-NSP
Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP
Windows_10	If Any	and Windows 10 (All)	and Condition(s)	then AnyConnect Configuration
Windows	If Any	and Windows All	and Condition(s)	then CiscoTemporalAgentWindows 4.7.00135 And WinSPWizard 2.5.0.1 And Cisco-ISE-NSP
MAC OS	If Any	and Mac OSX	and Condition(s)	then CiscoTemporalAgentOS X 4.7.00135 And MacOsXSPWizard 2.1.0.42 And Cisco-ISE-NSP
Chromebook	If Any	and Chrome OS All	and Condition(s)	then Cisco-ISE-Chrome-NSP

Save Reset

## 7. Créer une condition de posture

A. Accédez à "Règle > Eléments de règle > Conditions > Position > Condition de fichier"

B. Cliquez sur "Ajouter" et configurez le nom de condition "VPN\_Posture\_File\_Check", le système d'exploitation requis "Windows 10(All)", le type de fichier "FileExistence", le chemin d'accès au fichier "ABSOLUTE\_PATH" et le chemin d'accès complet et le nom de fichier "C:\custom.txt", sélectionnez l'opérateur de fichier "Exists"

c. Cet exemple utilise la présence d'un fichier nommé « custom.txt » sous le lecteur C : comme condition de fichier

**File Conditions List > VPN\_Posture\_File\_Check**

**File Condition**

\* Name: VPN\_Posture\_File\_Check

Description:

\* Operating System: Windows 10 (All)

Compliance Module: Any version

\* File Type: FileExistence

\* File Path: ABSOLUTE\_PATH

\* File Operator: Exists

C:\custom.txt

Save Reset

## 8. Créer une action de correction de posture

Accédez à "Stratégie > Eléments de stratégie > Résultats > Posture > Actions correctives" pour créer l'action corrective de fichier correspondante. Ce document utilise "Message Text Only" comme Actions correctives qui est configuré dans l'étape suivante.

## 9. Créer une règle de condition de posture

A. Accédez à "Stratégie > Eléments de stratégie > Résultats > Position > Exigences"

B. Cliquez sur Modifier, puis sélectionnez Insérer un nouveau besoin.

C. Configurez le nom de condition « VPN\_Posture\_Requirement », le système d'exploitation requis « Windows 10(All) », le module de conformité « 4.x ou ultérieur », le type de posture « Anyconnect »

D. Conditions comme "VPN\_Posture\_File\_Check" (créé à l'étape 7) et sous Actions correctives, sélectionnez Action comme "Texte du message uniquement" et entrez le message personnalisé pour l'utilisateur de l'agent

Name	Operating System	Compliance Module	Posture Type	Conditions	Remediations Actions
Default_Hardware_Attributes_Requirement_Mac	for Mac OSX	using 4.x or later	using AnyConnect	met if Hardware_Attributes_Check	then Select Remediations
Default_Firewall_Requirement_Win	for Windows All	using 4.x or later	using AnyConnect	met if Default_Firewall_Condition_Win	then Default_Firewall_Remediation_Win
Default_Firewall_Requirement_Mac	for Mac OSX	using 4.x or later	using AnyConnect	met if Default_Firewall_Condition_Mac	then Default_Firewall_Remediation_Mac
USB_Block_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if USB_Check	then Message Text Only
Any_AM_Installation_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if ANY_am_win_inst	then Message Text Only
Any_AM_Installation_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if ANY_am_mac_inst	then Message Text Only
Default_AppVis_Requirement_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if Default_AppVis_Condition_Win	then Select Remediations
Default_AppVis_Requirement_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if Default_AppVis_Condition_Mac	then Select Remediations
Default_Hardware_Attributes_Requirement_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if Hardware_Attributes_Check	then Select Remediations
Default_Hardware_Attributes_Requirement_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if Hardware_Attributes_Check	then Select Remediations
Default_Firewall_Requirement_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if Default_Firewall_Condition_Win	then Default_Firewall_Remediation_Win
Default_Firewall_Requirement_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if Default_Firewall_Condition_Mac	then Default_Firewall_Remediation_Mac
VPN_Posture_Requirement	for Windows 10 (All)	using 4.x or later	using AnyConnect	met if VPN_Posture_File_Check	then Message Text Only

Note: Remediation Action is filtered based on the operating system and stealth mode selection. Remediation Actions are not applicable for Application Conditions (configured using the Provision By Category or Provision By Everything options), Hardware Conditions, and External Data source conditions.

Save Reset

## 10. Créer une politique de posture

A. Accédez à "Politiques > Posture"

B. Configurez le nom de la règle sur « VPN\_Posture\_Policy\_Win », le système d'exploitation

requis sur « Windows 10(All) », le module de conformité sur « 4.x ou ultérieur », le type de posture sur « Anyconnect » et la configuration requise sur « VPN\_Posture\_Requirement », comme configuré à l'étape 9

Status	Policy Options	Rule Name	Identity Groups	Operating Systems	Compliance Module	Posture Type	Other Conditions	Requirements
2	Policy Options	Default_AppVis_Policy_Win	Any	Windows All	4.x or later	AnyConnect		Default_AppVis_Requirement_Win
2	Policy Options	Default_AppVis_Policy_Win_temporal	Any	Windows All	4.x or later	Temporal Agent		Default_AppVis_Requirement_Win_temporal
2	Policy Options	Default_Firewall_Policy_Mac	Any	Mac OSX	4.x or later	AnyConnect		Default_Firewall_Requirement_Mac
2	Policy Options	Default_Firewall_Policy_Mac_temporal	Any	Mac OSX	4.x or later	Temporal Agent		Default_Firewall_Requirement_Mac_temporal
2	Policy Options	Default_Firewall_Policy_Win	Any	Windows All	4.x or later	AnyConnect		Default_Firewall_Requirement_Win
2	Policy Options	Default_Firewall_Policy_Win_temporal	Any	Windows All	4.x or later	Temporal Agent		Default_Firewall_Requirement_Win_temporal
2	Policy Options	Default_Hardware_Attributes_Policy_Mac	Any	Mac OSX	4.x or later	AnyConnect		Default_Hardware_Attributes_Requirement_Mac
2	Policy Options	Default_Hardware_Attributes_Policy_Mac_temporal	Any	Mac OSX	4.x or later	Temporal Agent		Default_Hardware_Attributes_Requirement_Mac_temporal
2	Policy Options	Default_Hardware_Attributes_Policy_Win	Any	Windows All	4.x or later	AnyConnect		Default_Hardware_Attributes_Requirement_Win
2	Policy Options	Default_Hardware_Attributes_Policy_Win_temporal	Any	Windows All	4.x or later	Temporal Agent		Default_Hardware_Attributes_Requirement_Win_temporal
2	Policy Options	Default_USB_Block_Policy_Win	Any	Windows All	4.x or later	AnyConnect		USB_Block
2	Policy Options	Default_USB_Block_Policy_Win_temporal	Any	Windows All	4.x or later	Temporal Agent		USB_Block_temporal
2	Policy Options	VPN_Posture_Policy_Win	Any	Windows 10 (All)	4.x or later	AnyConnect		VPN_Posture_Requirement

## 11. Créer des listes de contrôle d'accès dynamiques

Accédez à "Policy > Policy Elements > Results > Authorization > Downloadable ACLs" et créez les DACL pour différents états de position.

Ce document utilise les DACL suivantes.

### A. Posture Unknown : autorise le trafic vers DNS, PSN, HTTP et HTTPS

Downloadable ACL List > PostureUnknown

**Downloadable ACL**

\* Name: PostureUnknown

Description: [Empty]

IP version:  IPv4  IPv6  Agnostic

\* DAACL Content:

```

1234567 permit udp any any eq domain
8910111 permit ip any host 10.106.44.77
2131415 permit tcp any any eq 80
1617181 permit tcp any any eq 443
9202122
2324252
6272829
3031323
3343536
    
```

Check DAACL Syntax

Save Reset



## B. Posture non conforme : refuse l'accès aux sous-réseaux privés et autorise uniquement le trafic Internet

The screenshot shows the configuration page for a Downloadable ACL in Cisco ISE. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The left sidebar shows the navigation menu with 'Authorization' > 'Downloadable ACLs' selected. The main content area is titled 'Downloadable ACL List > PostureNonCompliant'. The configuration details are as follows:

- Name:** PostureNonCompliant
- Description:** (empty field)
- IP version:** IPv4 (selected), IPv6, Agnostic
- DACL Content:**

```
1234567 deny ip any 10.0.0.0 255.0.0.0
8910111 deny ip any 172.16.0.0 255.240.0.0
2131415 deny ip any 192.168.0.0 255.255.0.0
1617181 permit ip any any
9202122
2324252
6272829
3031323
3343536
```
- Buttons:** Save, Reset

## C. Conformité à la position : autorise tout le trafic pour les utilisateurs finaux conformes à la position

The screenshot shows the configuration page for a Downloadable ACL in Cisco ISE. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The left sidebar shows the navigation menu with 'Authorization' > 'Downloadable ACLs' selected. The main content area is titled 'Downloadable ACL List > PostureCompliant'. The configuration details are as follows:

- Name:** PostureCompliant
- Description:** (empty field)
- IP version:** IPv4 (selected), IPv6, Agnostic
- DACL Content:**

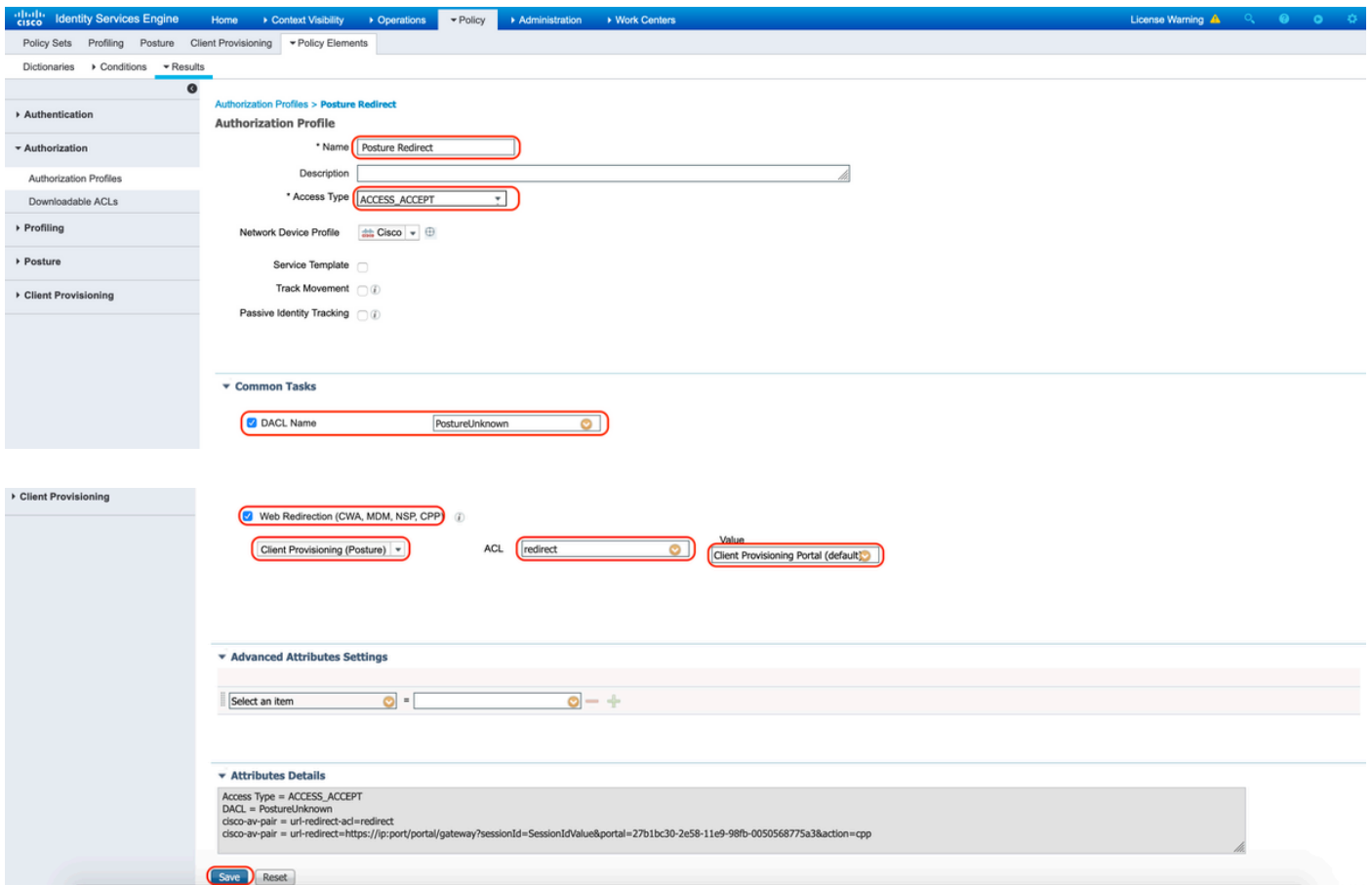
```
1234567 permit ip any any
8910111
2131415
1617181
9202122
2324252
6272829
3031323
3343536
```
- Buttons:** Save, Reset

## 12. Créer des profils d'autorisation

Accédez à "Stratégie > Eléments de stratégie > Résultats > Autorisation > Profils d'autorisation".

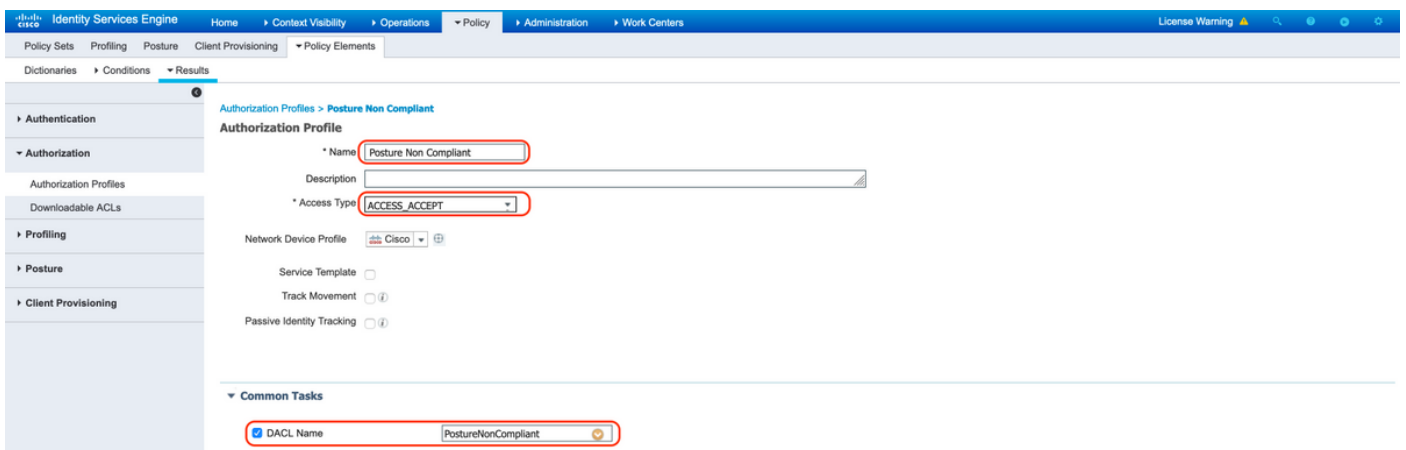
### A. Profil d'autorisation pour une posture inconnue

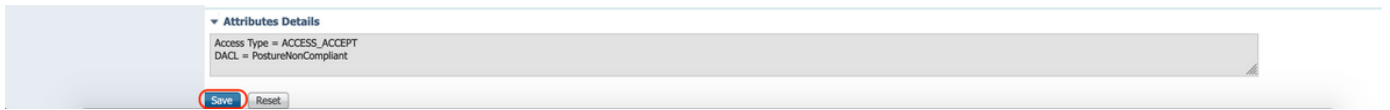
Sélectionnez DACL « PostureUnknown », cochez Redirection Web, sélectionnez Provisioning client (Posture), configurez Redirect ACL name « redirect » (à configurer sur ASA), puis sélectionnez le portail Provisioning client (par défaut)



## B. Profil d'autorisation pour posture non conforme

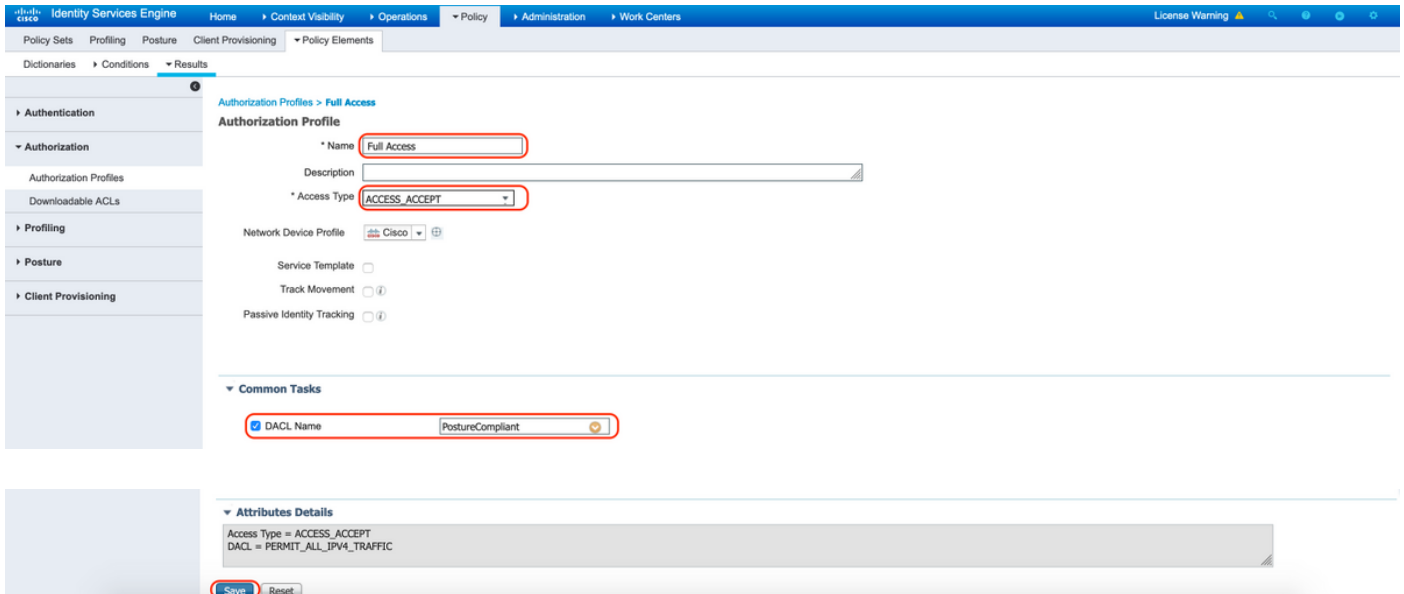
Sélectionnez DACL "PostureNonCompliant" pour limiter l'accès au réseau





## C. Profil d'autorisation de conformité à la posture

Sélectionnez DAACL « PostureCompliant » pour autoriser un accès complet au réseau



## 12. Configurer les stratégies d'autorisation

Utilisez les profils d'autorisation configurés à l'étape précédente pour configurer 3 stratégies d'autorisation pour les états Conformité à la position, Non-conformité à la position et Inconnu à la position.

La condition commune « Session : État de la position » est utilisée pour déterminer les résultats de chaque stratégie

The screenshot shows the Cisco ISE Policy Sets configuration interface. The 'Policy Sets' menu is selected, and the 'Default' policy set is highlighted. The 'Authorization Policy (15)' section is expanded, showing three rules:

Status	Rule Name	Conditions	Results	Security Groups	Hits	Actions
✓	Anyconnect Posture Compliant	Session PostureStatus EQUALS Compliant	Full Access	Select from list	6	Settings
✓	Anyconnect Posture Non Compliant	Session PostureStatus EQUALS NonCompliant	Posture Non Compliant	Select from list	0	Settings
✓	Anyconnect Posture Unknown	AND Network Access-Device IP Address EQUALS 10.197.164.3 Session PostureStatus EQUALS Unknown	Posture Redirect	Select from list	13	Settings

## Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Pour vérifier si l'utilisateur est authentifié avec succès, exécutez la commande suivante sur l'ASA.

```
<#root>
```

```
firebird(config)#
```

```
show vpn-sess detail anyconnect
```

Session Type: AnyConnect Detailed

```
Username      : _585b5291f01484dfd16f394be7031d456d314e3e62
Index         : 125
Assigned IP   : explorer.cisco.com      Public IP    : 10.197.243.143
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
Hashing       : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Bytes Tx      : 16404                   Bytes Rx     : 381
Pkts Tx       : 16                       Pkts Rx     : 6
Pkts Tx Drop  : 0                         Pkts Rx Drop : 0
Group Policy  : DfltGrpPolicy              Tunnel Group :
```

TG\_SAML

```
Login Time    : 07:05:45 UTC Sun Jun 14 2020
Duration      : 0h:00m:16s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                       VLAN         : none
```

Audt Sess ID : 0ac5a4030007d0005ee5cc49  
Security Grp : none

AnyConnect-Parent Tunnels: 1  
SSL-Tunnel Tunnels: 1  
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:

Tunnel ID : 125.1  
Public IP : 10.197.243.143  
Encryption : none Hashing : none  
TCP Src Port : 57244 TCP Dst Port : 443  
Auth Mode : SAML  
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes  
Client OS : win  
Client OS Ver: 10.0.15063  
Client Type : AnyConnect  
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052  
Bytes Tx : 7973 Bytes Rx : 0  
Pkts Tx : 6 Pkts Rx : 0  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 125.2  
Assigned IP : explorer.cisco.com Public IP : 10.197.243.143  
Encryption : AES-GCM-256 Hashing : SHA384  
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384  
Encapsulation: TLSv1.2 TCP Src Port : 57248  
TCP Dst Port : 443 Auth Mode : SAML  
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes  
Client OS : Windows  
Client Type : SSL VPN Client  
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052  
Bytes Tx : 7973 Bytes Rx : 0  
Pkts Tx : 6 Pkts Rx : 0  
Pkts Tx Drop : 0 Pkts Rx Drop : 0  
Filter Name : #ACSACL#-IP-PostureUnknown-5ee45b05

DTLS-Tunnel:

Tunnel ID : 125.3  
Assigned IP : explorer.cisco.com Public IP : 10.197.243.143  
Encryption : AES-GCM-256 Hashing : SHA384  
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384  
Encapsulation: DTLSv1.2 UDP Src Port : 49175  
UDP Dst Port : 443 Auth Mode : SAML  
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes  
Client OS : Windows  
Client Type : DTLS VPN Client  
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052  
Bytes Tx : 458 Bytes Rx : 381  
Pkts Tx : 4 Pkts Rx : 6  
Pkts Tx Drop : 0 Pkts Rx Drop : 0  
Filter Name :

#ACSACL#-IP-PostureUnknown-5ee45b05

ISE Posture:

Redirect URL : <https://ise261.pusaxena.local:8443/portal/gateway?sessionId=0ac5a4030007d0005ee5cc49&pc>  
Redirect ACL : redirect

Une fois l'évaluation de la position terminée, l'accès utilisateur est remplacé par un accès complet, comme observé dans la liste de contrôle d'accès dynamique insérée dans le champ « Nom du filtre »

<#root>

firebird(config)#

show vpn-sess detail anyconnect

Session Type: AnyConnect Detailed

Username : \_585b5291f01484dfd16f394be7031d456d314e3e62  
Index : 125  
Assigned IP : explorer.cisco.com Public IP : 10.197.243.143  
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel  
License : AnyConnect Premium  
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256  
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384  
Bytes Tx : 16404 Bytes Rx : 381  
Pkts Tx : 16 Pkts Rx : 6  
Pkts Tx Drop : 0 Pkts Rx Drop : 0  
Group Policy : DfltGrpPolicy Tunnel Group :

TG\_SAML

Login Time : 07:05:45 UTC Sun Jun 14 2020  
Duration : 0h:00m:36s  
Inactivity : 0h:00m:00s  
VLAN Mapping : N/A VLAN : none  
Audt Sess ID : 0ac5a4030007d0005ee5cc49  
Security Grp : none

AnyConnect-Parent Tunnels: 1  
SSL-Tunnel Tunnels: 1  
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:

Tunnel ID : 125.1  
Public IP : 10.197.243.143  
Encryption : none Hashing : none  
TCP Src Port : 57244 TCP Dst Port : 443  
Auth Mode : SAML  
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes  
Client OS : win  
Client OS Ver: 10.0.15063  
Client Type : AnyConnect  
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052  
Bytes Tx : 7973 Bytes Rx : 0  
Pkts Tx : 6 Pkts Rx : 0  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 125.2  
Assigned IP : explorer.cisco.com Public IP : 10.197.243.143  
Encryption : AES-GCM-256 Hashing : SHA384

Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384  
 Encapsulation: TLSv1.2 TCP Src Port : 57248  
 TCP Dst Port : 443 Auth Mode : SAML  
 Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes  
 Client OS : Windows  
 Client Type : SSL VPN Client  
 Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052  
 Bytes Tx : 7973 Bytes Rx : 0  
 Pkts Tx : 6 Pkts Rx : 0  
 Pkts Tx Drop : 0 Pkts Rx Drop : 0  
 Filter Name : #ACSACL#-IP-PERMIT\_ALL\_IPV4\_TRAFFIC-57f6b0d3

**DTLS-Tunnel:**

Tunnel ID : 125.3  
 Assigned IP : explorer.cisco.com Public IP : 10.197.243.143  
 Encryption : AES-GCM-256 Hashing : SHA384  
 Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384  
 Encapsulation: DTLSv1.2 UDP Src Port : 49175  
 UDP Dst Port : 443 Auth Mode : SAML  
 Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes  
 Client OS : Windows  
 Client Type : DTLS VPN Client  
 Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052  
 Bytes Tx : 458 Bytes Rx : 381  
 Pkts Tx : 4 Pkts Rx : 6  
 Pkts Tx Drop : 0 Pkts Rx Drop : 0  
 Filter Name :

#ACSACL#-IP-PERMIT\_ALL\_IPV4\_TRAFFIC-57f6b0d3

Pour vérifier si l'autorisation a été correctement effectuée sur ISE, accédez à **Operations > RADIUS > Live Logs**

Cette section présente les informations pertinentes associées à l'utilisateur autorisé, c'est-à-dire l'identité, le profil d'autorisation, la politique d'autorisation et le statut.

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorization Pro...	Posture St...	IP Address	Network Device
Jun 14, 2020 07:44:59.975 AM			0	_585b5291f01484d1d1...	00:50:56:A0:D6:97	Windows10-...	Default	Anyconnect ...	Full Access	Compliant	10.197.164.7	ASA
Jun 14, 2020 07:44:59.975 AM				#ACSACL#-IP-PERMI...								ASA
Jun 14, 2020 07:44:34.963 AM				#ACSACL#-IP-Posture...								ASA
Jun 14, 2020 07:44:34.958 AM				_585b5291f01484d1d1...	00:50:56:A0:D6:97	Windows10-...	Default	Default >> A...	Posture Redirect	Pending		ASA


**Remarque :** pour plus d'informations sur la validation de posture sur ISE, reportez-vous à la documentation suivante :

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215236-ise-posture-over-anyconnect-remote-acces.html#anc7>

Pour vérifier l'état d'authentification sur le portail d'administration Duo, cliquez sur « Rapports » sur le côté gauche du panneau d'administration qui affiche le journal d'authentification.

Plus de détails : <https://duo.com/docs/administration#reports>

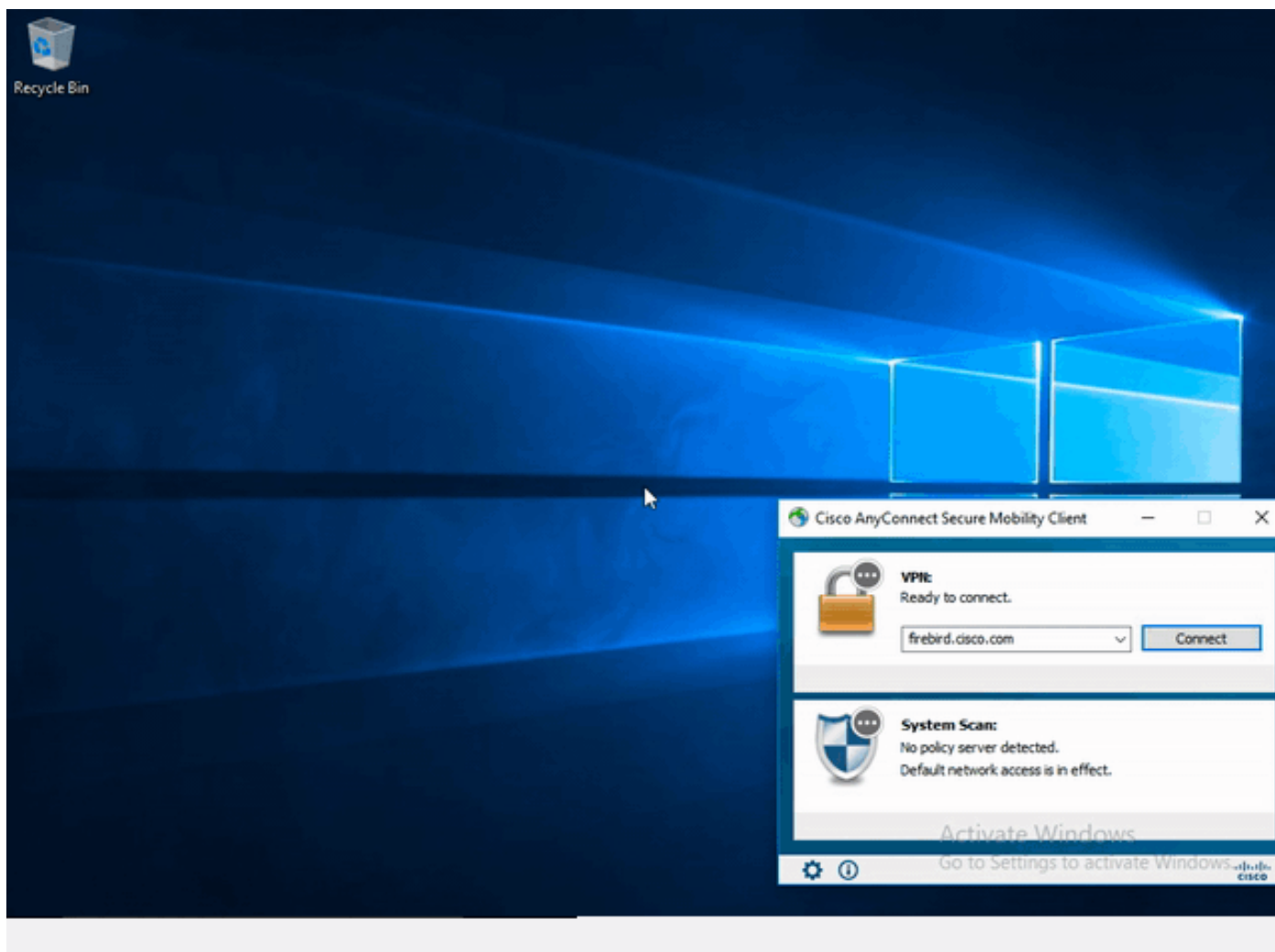
---

 Pour afficher la journalisation du débogage pour la passerelle d'accès Duo, utilisez le lien suivant :

[https://help.duo.com/s/article/1623?language=en\\_US](https://help.duo.com/s/article/1623?language=en_US)

---


## Expérience utilisateur



## Dépannage

Cette section fournit les informations que vous pouvez utiliser afin de dépanner votre configuration.


---

 Remarque : Consulter les renseignements importants sur les commandes de débogage avant d'utiliser les commandes de débogage.

---



---

 Attention : sur l'ASA, vous pouvez définir différents niveaux de débogage ; par défaut, le niveau 1 est utilisé. Si vous modifiez le niveau de débogage, le niveau de détail des débogages peut augmenter. Faites-le avec prudence, en particulier dans les environnements de production.

---

La plupart des dépannages SAML impliquent une mauvaise configuration qui peut être trouvée en vérifiant la configuration SAML ou en exécutant des débogages.

"debug webvpn saml 255" peut être utilisé pour dépanner la plupart des problèmes, cependant dans les scénarios où ce débogage ne fournit pas d'informations utiles, des débogages supplémentaires peuvent être exécutés :


```
debug webvpn 255
debug webvpn anyconnect 255
debug webvpn session 255
debug webvpn request 255
```

Pour résoudre les problèmes d'authentification et d'autorisation sur ASA, utilisez les commandes debug suivantes :

```
debug radius all
debug aaa authentication
debug aaa authorization To troubleshoot Posture related issues on ISE, set the following attributes to
```

```
posture (ise-psc.log)
portal (guest.log)
provisioning (ise-psc.log)
runtime-AAA (prrt-server.log)
nsf (ise-psc.log)
nsf-session (ise-psc.log)
swiss (ise-psc.log)
```

---

 Remarque : pour obtenir des informations détaillées sur le flux de posture et le dépannage d'AnyConnect et d'ISE, reportez-vous au lien suivant :

[Comparaison des styles de posture ISE pour Pre et Post 2.2](#)

Pour interpréter et dépanner les journaux de débogage de Duo Access Gateway

---

## Informations connexes

<https://www.youtube.com/watch?v=W6bE2GTU0Is&>

<https://duo.com/docs/cisco#asa-ssl-vpn-using-saml>

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215236-ise-posture-over-anyconnect-remote-acces.html#anc0>

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.